

**REMARKS**

This Amendment and the following remarks are intended to fully respond to the Office Action mailed March 22, 2007. In that Office Action, claims 1-30 were examined and all claims were rejected. Claims 1-3, 5-13, 15-23, and 25-30 were rejected under 35 U.S.C. ¶ 102(e) as being anticipated by Cannon et al. (US 2004/0010696) (“Cannon”). Claims 4, 14, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cannon in view of Seamons et al. (US 2002/0016777) (“Seamons”). In this Response, claims 1, 7-11, and 17-21 have been amended; and no claims have been added or canceled. Therefore, claims 1-30 remain present for examination.

**Cannon does not anticipate all of the limitations of any claim.**

Cannon is directed to a system and method for authenticating a user to a transacting entity. A user employs an identification device, such as a fingerprint machine, to obtain sample biometric data about the user (such as a digital representation of the user’s fingerprint). *See* Cannon, Para. 0057. The sample biometric data is combined with “identity data” in a “print document” that is forwarded to a terminal. *See* Cannon, Para. 0057-0058. The terminal, or a separate identification service provider (IDSP), attempts to match the sample biometric data to reference biometric data. *See* Cannon, Para. 0060-0061. The reference biometric data is located using the identity data to look up the user’s previously stored reference biometric data for comparison. *See* Cannon, Para. 0064.

Accordingly, Cannon depends on a previous registration process that is not described. In other words, the user’s identity must already be established at the IDSP in Cannon so that the biometric data (such as the user’s fingerprint) can be compared against something. Cannon is not directed to, nor does it describe how to, establish a new identity at a receiving party. Rather, Cannon is directed to a system for confirming that a user is who he/she represents to be based on previously registered user data.

By contrast, the claimed systems and methods describe the establishment of an identity of a principal at a recipient, for example, where the principal has not previously registered identity information. Claims 1, 11 and 21, as amended, require a system or method of sending: “an

identity information document . . . to establish an identity of a principal at a recipient.” Cannon is not directed at the establishment of an identity at a recipient, but rather the confirmation that a user is who he/she claims to be based on previously established reference data.

Moreover, claims 1, 11, and 21 further require selecting “identity information from a self-identity information store for inclusion in the identity information document, wherein the selected identity information comprises a subset of identity information relating to the principal in the self-identity information store.” Cannon does not disclose “selecting” identity information from a self-identity information store. Although identity data may be combined with sample print data in Cannon to create a print document, there is no disclosure that such identity information is “selected” in any way. Nor is there any suggestion or disclosure in Cannon that the selected identity information is a “subset of identity information relating to the principal in the self-identity information store.”

By permitting the “selection” of a “subset” of identity information from the self-identity information store, the method and systems of claims 1, 11, and 21 permit a principal to effectively control the extent identity information is released to a recipient. Among other things, this permits a principal to store a variety of identity information about the principal for easy access but choose to selectively release such identity information only as needed to a particular recipient. For example, a principal may store ten pieces of personal information in the self-identity information store. A first recipient may require only three such pieces of information to establish an identity. If only those three pieces of information are selected and sent in an identity document to the recipient, the other seven pieces of information are effectively protected from the risk of unneeded disclosure.

The Examiner contends that in Cannon “by placing your fingers on the sensor, you are requesting the subset of info from memory corresponding to the respective print data.” *See* Office Action, Para. 6. Applicants respectfully disagree. Although identity data is attached to the digital representation of the user’s fingerprint, there is no disclosure that a “subset” of such identity data “relating to the principal” can be “selected” as required in claims 1, 11, and 21. Rather, without any further explanation in Cannon, it appears that whatever identity data is available on the identification device is simply included in the print document and forwarded to

the terminal. This does not meet the requirement for selective inclusion of a subset of stored identity information in an identity document.

For at least the foregoing reasons, claims 1, 11, and 21 are not anticipated by Cannon. Claims 2-6, 12-16, and 22-30 all depend on one of claims 1, 11, or 21, and are therefore also not anticipated by Cannon. Reconsideration of these rejections is respectfully requested.

In addition, with specific reference to claim 6, the user of the claimed method is further provided with control over his/her identity information by requiring that the selected identity information comprise: “use policies for defining uses to which the contents of the identity information may be put.” For example, a use policy may indicate other parties to which the identity information may be disclosed. *See* Specification, p. 22, reference number 606. The Examiner contends that this is disclosed in Cannon at paragraph 0065, lines 7-14 and Figure 8, item 602. Applicants respectfully disagree. The cited lines of paragraph 0065 simply have no relation to “use policies for defining uses to which the contents of the identity information may be put.” Similarly, item 602 in Figure 8 of Cannon includes print document module 820, sample print 802, identity 812, individual private key 814, and reference minutia 816. There is no disclosure in Cannon that any of these elements have anything to do with “use policies.” Claims 16 and 26 similarly require “use policies for defining uses to which the contents of the identity information may be put.” Reconsideration of these rejections is respectfully requested.

Independent claim 7, as amended, is directed to a method of receiving an identity document and requires both “saving the identity information in a recognized identity information store if the identity information is determined to be reliable” and “determining whether to verify the identity information if the identity information is not reliable.” At least the combination of these two steps is not present in Cannon. The Examiner contends that Cannon discloses determining whether the identity information is “reliable” in paragraph 0064, lines 9-19. The referenced section refers to the IDSP comparing the sample print data via a “triple match operation” to the reference print data. Even if this qualified as determining whether the identity information is “reliable” as used in Claim 7, the identity information that has been sent to the IDSP is not “saved” as a result. Rather, the result of a successful “triple match” is that the “[t]erminal 605 facilitates or enables the transaction between the user 601 and the transacting

entity 610.” *See* Cannon, Para. 0064. The Examiner cites Figure 8, item 890, for the proposition that Cannon saves “the identity information in a recognized identity information store if the identity information is determined to be reliable.” *See* Office Action, Para. 9. Database 890 in Figure 8, however, contains previously saved reference data, such as records 892 that are used to compare to sample data for approval of a transaction with transacting entity 610. *See* Cannon, Para. 0081. There is no disclosure in Cannon that a successful indication of reliability of the identity information results in saving the identity information in a recognized identity information store because Cannon has no need for a print document once the user’s fingerprint has been verified. Again, Cannon is directed to a different type of system – one where an identity for the user has already been established.

Moreover, the Examiner contends that paragraph 0065, lines 14-19 of Cannon meets the limitation of amended claim 7 that requires “determining whether to verify the identity information if the identity information is not reliable.” Again, Applicants respectfully disagree. The recited section in Cannon is referring to the same determination of whether the sample print data matches the reference print data. Effectively, it is the same step the Examiner cited for the determination whether the identity information is reliable. In claim 7, the determination whether the identity information is reliable is a separate step from the determination whether to verify the identity information if the identity information is not reliable. Without limitation, in embodiments, the present specification describes the determination of reliability as a first step that could be performed by a user of a recipient system. For example, if the user of a recipient system knows that the identity information that was received was reliable, he could simply accept it and save the identity information into the “recognized identity information store.” *See*, e.g., Specification, pp. 18-19. If the determination is made that the information is not reliable (e.g., the user of the recipient system cannot define it as reliable), then a determination is made whether to attempt to verify the information. This can occur, in embodiments, by verifying the identity information through another channel. *See*, e.g., Specification, pp. 19-20.

Cannon simply contains no disclosure of these steps of claim 7 in combination. Claim 17 similarly requires instructions to: “determine whether identity information in the identity information document is reliable, determine whether to verify the identity information if the identity information is not reliable, and save the identity information in a recognized identity

information store if the identity information is determined to be reliable.” Accordingly, Cannon does not anticipate all of the limitations of claims 7 and 17. Claims 8-10 and 18-20 depend on claim 7 or 17 and are similarly allowable. Reconsideration of these rejections is respectfully requested.

In addition, with specific reference to claims 8, 18, and 28, Cannon also does not disclose the use of an identification recognition number in the manner claimed. The Examiner again cites the Boolean determination of whether trust exists between the user and the transacting entity based on a match between the user’s sample print and the reference print. This simply has nothing to do with using an IRN to verify identity information if the identity information is first not deemed reliable. Reconsideration of these rejections is also respectfully requested.

**Seamons does not make up for the deficiencies of Cannon.**

Claims 4, 14, and 24 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Cannon in view of Seamons et al. (US 2002/0016777) (“Seamons”). In light of the amendments and response set forth above, and because claims 4, 14, and 24 all depend upon otherwise allowable claims, it is believed that this rejection is now moot, and reconsideration is respectfully requested. Neither Seamons nor any other cited art cures the deficiencies of Cannon discussed above.

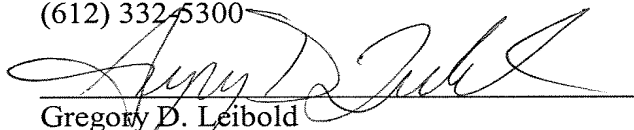
**Conclusion**

It is believed that no further fees are due with this Response. However, the Commissioner is hereby authorized to charge any deficiencies or credit any overpayment with respect to this patent application to deposit account number 13-2725.

In light of the above remarks and amendments, it is believed that the application is now in condition for allowance and such action is respectfully requested. Should any additional issues need to be resolved, the Examiner is requested to telephone the undersigned to attempt to resolve those issues.

Respectfully submitted,  
MERCHANT & GOULD P.C.  
P.O. Box 2903  
Minneapolis, Minnesota 55402-0903  
(612) 332-5300

Date: June 22, 2007

  
Gregory D. Leibold  
Reg. No. 36,408

